Semantics of Security

Presented at

SSTC 2006

3 May 2006

Paul Shaw
Navy Command and Control
Functional Data Manager
paul.shaw@navy.mil

Abstract

This presentation explores semantics as an enabling technology to solve the daunting security problems of preparation and response as applied to Maritime Domain Awareness (MDA). Maritime Security depends upon the fusion of intelligence across thousands of diverse organizations (International, Federal, State, Local, and Commercial), processing large volumes of information, and interconnecting multitudes of sensors and systems.   Traditional methods for interoperability and data exchange will not achieve the desired coordination between agencies, especially to prevent and/or respond to a major incident (natural disaster or terrorist attack). Ontologies, machine-processable semantics, will be examined for their ability to solve interoperability problems and provide predictive analytics for MDA missions. Additionally, management and development of the semantic web and MDA semantic layers will be discussed.

Objectives:
- How ontolgies would assist the Maritime Security Problem
- What are the data quality attributes that will allow creation of data context
- A Framework for the development of MDA Semantic Layer
- Emphasis on data security as an element of data context
- How System of System (SoS) methodologies can develop required ontologies

Maritime Security Problem

Maritime Domain Awareness (MDA) **... Maximizing awareness of security issues in the maritime domain in order to support U. S. forces and improve United States Government actions in response to identified threats (*NSPD 41*, p. 2)* ... It is critical that the United States *develop an enhanced capability to identify threats* to the maritime domain as early and as distant from our shores as possible. (*NSPD-41*, p.5)***

- **Maritime security response and counterterrorism operations**
- **Maritime intercept operations**
- **Prevention and detection of, and response to, mining of U.S. ports**
- **Detection, interdiction and disposition of targeted cargo, people, and vessels**
- **Attacks on vessels with U. S. citizens aboard or that effect U. S. interests anywhere in the world**

* National Security Presidential Directive NSPD-41
Homeland Security Presidential Directive HSPD-13,
The White House, December 21, 2004
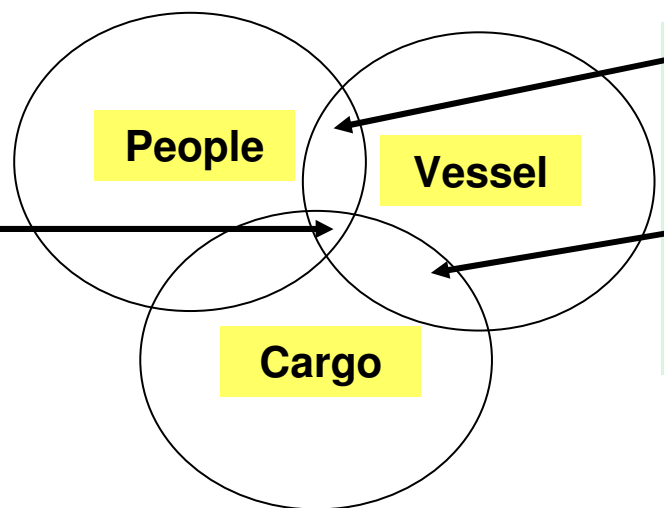
Scope of the Maritime Data Management

Describe the initial community vocabulary that is necessary to Maritime Security.

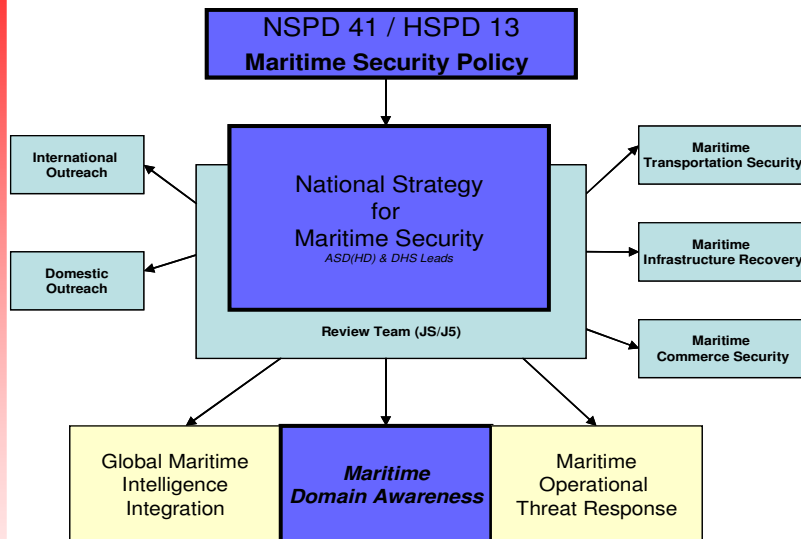Maritime Situation Awareness (SA):

What, When, Where, and Why?

Consider data related to people, vessels, and cargo…?

Consider three-way overlap for initial common vocabulary definition, spiral 1. Results in the initial schema.

Consider two-way overlaps for follow-on common vocabulary definition, spiral 2.

Results in extensions to the initial schema.

People

Vessel

Cargo

Data Strategy Requirement

NSPD 41 / HSPD 13
Maritime Security Policy

International Outreach

Domestic Outreach

National Strategy
for
Maritime Security
ASD(HD) & DHS Leads

Review Team (JS/J5)

Maritime Transportation Security

Maritime Infrastructure Recovery

Maritime Commerce Security

Global Maritime Intelligence Integration

Maritime Domain Awareness

Maritime Operational Threat Response

Maritime Domain Awareness (MDA) is effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States …

Understanding the Complexity

- **On-demand Data Access**
  - Understanding of anything associated with global maritime domain
- **Managing Uncertainty**
  - Threat vs. Capability Based Response Plan
- **COI to COI Integration**
  - No established Core COI Structure (data or processes) to leverage

Goal: Improve our ability to *collect, fuse, analyze, display, and disseminate* actionable information and intelligence to the operational commander.

On-demand Data Requirement

Maritime Domain Awareness (MDA) **is effective** *understanding of anything associated* *with the global maritime domain* **that could impact the security, safety, economy, or environment of the United States (*NSPD-41*, p. 5).... It will be achieved by improving our ability to collect, fuse, analyze, display, and disseminate** actionable information and intelligence **to operational commanders.**
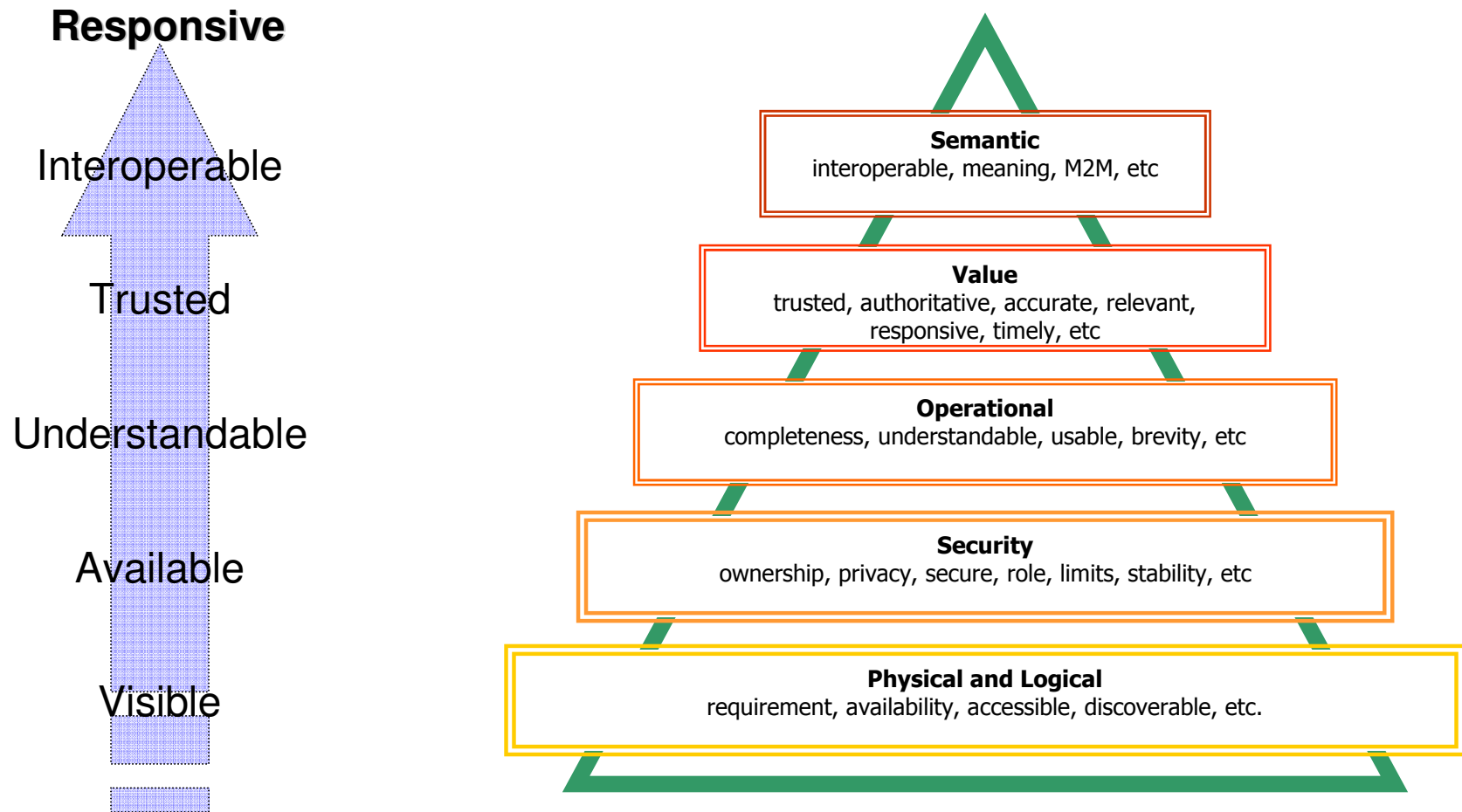
In other words; *Right data, right place, right time, all the time.*

This implies the "right" data:

- Exists,

- Is visible (i.e., discoverable),

- Is accessible

- Is understandable

- Is trusted

DoD 8320.2-G Guidance to COIs for Implementing Net-Centric Information Sharing, dated November 7, 2005.

Hierarchy of Data Needs

Responsive

Interoperable

Trusted

Understandable

Available

Visible

Semantic
interoperable, meaning, M2M, etc

Value
trusted, authoritative, accurate, relevant, responsive, timely, etc

Operational
completeness, understandable, usable, brevity, etc

Security
ownership, privacy, secure, role, limits, stability, etc

Physical and Logical
requirement, availability, accessible, discoverable, etc.

****Modified from Maslow's Hierarchy of Needs
(original five-stage model)**

DoD 8320.2-G Guidance to COIs for Implementing Net-Centric Information Sharing, dated November 7, 2005.

Data Understandability

Net Centricity: DoD is moving to a net-centric environment in which all elements of the DoD are able to seamlessly share information, resulting in dramatic improvements in combat power and decision superiority.

Data Understandability Elements

- A context for the information can be understood
- Metadata (e.g. XML), which provides a way to describe data assets and the use of registries, catalogs, and shared spaces
- Mechanisms to understand data context
- Discoverable Services that enable data tagging, sharing, searching, and retrieving
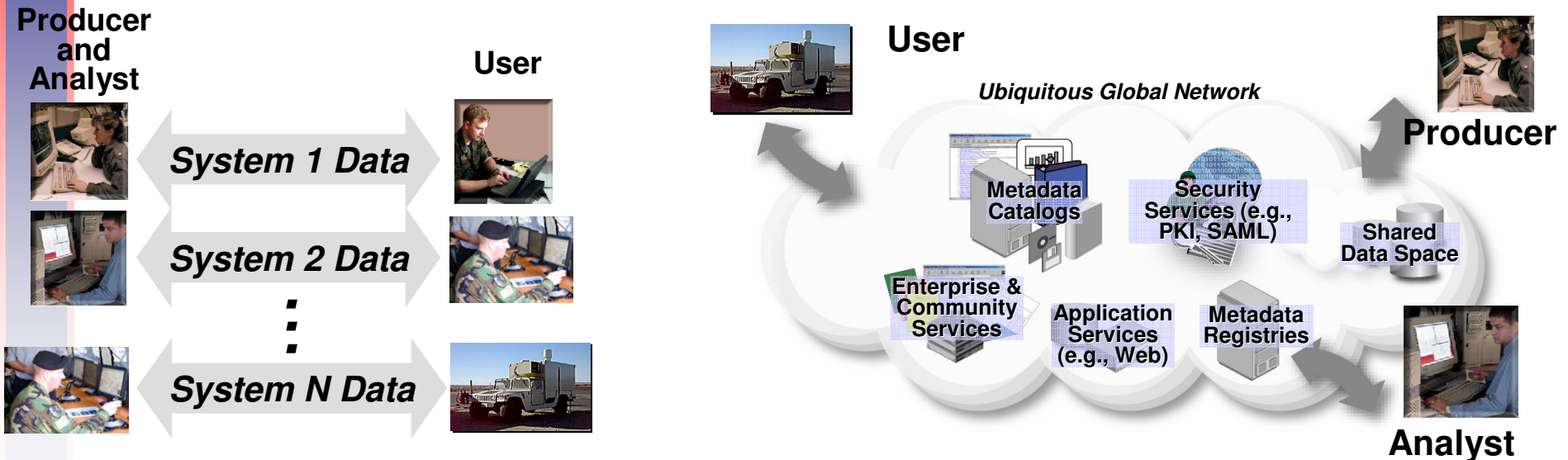
Net Centricity Wants Information

- **Joint Chiefs of Staff (JCS) Joint Pub 6-0 (<u>Doctrine for Command, Control, Communications and Computer (C4) Systems Support to Joint Operations</u>) describes data with a combination of seven information quality criteria (JCS Joint Pub 6-0 Page 1-5) as usable information:**

    - **Accuracy - Information conveys the true situation**

    - **Relevance - Information applies to the mission**

    - **Timeliness - Information that is available in time to make the decision**

    - **Usability - Information that is in common, easily understood format and displays**

    - **Completeness - All necessary information is required by the decision maker**

    - **Brevity - Information only has the level of detail required**

    - **Security - Information that has been afforded adequate protection where required**

"Information is data collected from the environment and processed into a usable form" (JCS Pub 6-0 page 1-3)

Net-Centricity Depends Upon a Data Strategy

Under Net Centricity, Data is to be:

- **Visible, Accessible, and _Understandable_**
- **Shared to supports planned and unplanned consumers**
- **Have a _shared meaning_ for understanding (independent of System)**

Producer and Analyst

User

System 1 Data

System 2 Data

System N Data

User

Ubiquitous Global Network

Metadata Catalogs

Security Services (e.g., PKI, SAML)

Producer

Shared Data Space

Enterprise & Community Services

Application Services (e.g., Web)

Metadata Registries
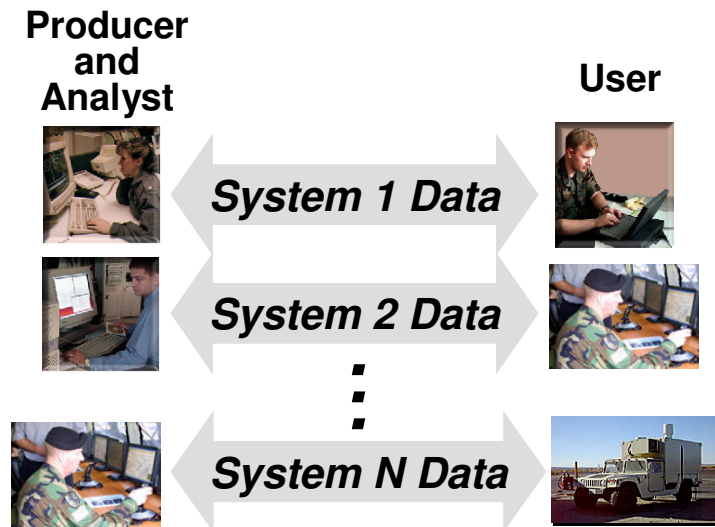
Analyst

From _System centric:_
- Multiple systems to find data
- Private data – only supports user of system
- User translates data as needed for mission accomplishment across multiple sources

To _Net Centric:_
- Data is visible, accessible and understandable
- Shared data – supports planned and unplanned consumers
- Shared meaning of the data enables understanding for a given purpose

Pre-Net-centric: User

- ## User concerned with:
  - ### Usable,
  - ### Brief (Appropriate level of detail), and
  - ### Timely

- ## User assumed:
  - ### Relevant
  - ### Accurate
  - ### Complete
  - ### Secure

Producer and Analyst

User

System 1 Data

System 2 Data

:

System N Data

From _System centric:_
- Multiple systems to find data
- Private data – only supports user of system
- User translates data as needed for mission accomplishment across multiple sources

The burden was on the User to transform "Data" into "Mission Information"
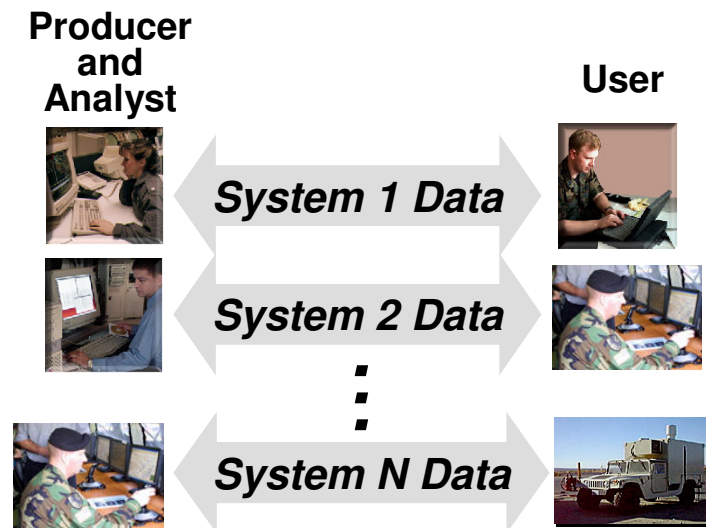
Pre-Net-centric: Analyst

- ## Analyst concerned with:
    - ### Relevant
    - ### Accurate
    - ### Complete
    - ### Secure

- ## Analyst traded off:
    - ### Usability
    - ### Timeliness
    - ### Brevity

Producer and Analyst

User

System 1 Data

System 2 Data
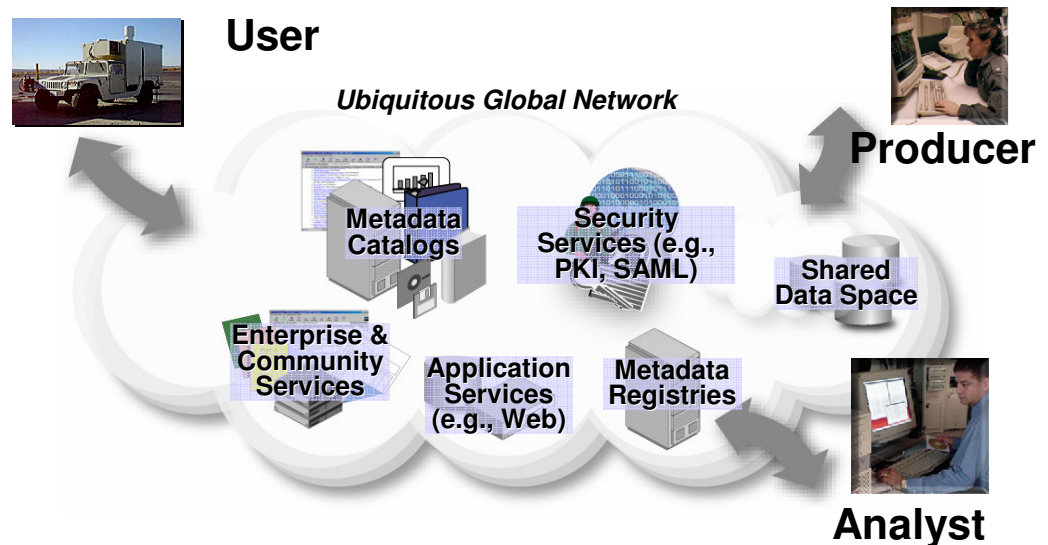
System N Data

From _System centric:_
- Multiple systems to find data
- Private data – only supports user of system
- User translates data as needed for mission accomplishment across multiple sources

The Analyst processed "Data" to create "Mission Information"

Net-Centric

- **"Data" to "Mission Information":**
  - **Brief**
  - **Timely**
  - **Usable**
  - **Relevant**
  - **Accurate**
  - **Complete**
  - **Secure**

User

Ubiquitous Global Network

Metadata Catalogs

Security Services (e.g., PKI, SAML)

Enterprise & Community Services

Application Services (e.g., Web)

Metadata Registries

Producer

Shared Data Space

Analyst

To *Net Centric:*
- Data is visible, accessible and understandable
- Shared data – supports planned and unplanned consumers
- Shared meaning of the data enables understanding for a given purpose

MDA Data Strategy strives to automate the transformation of "Data" to "Mission Information"
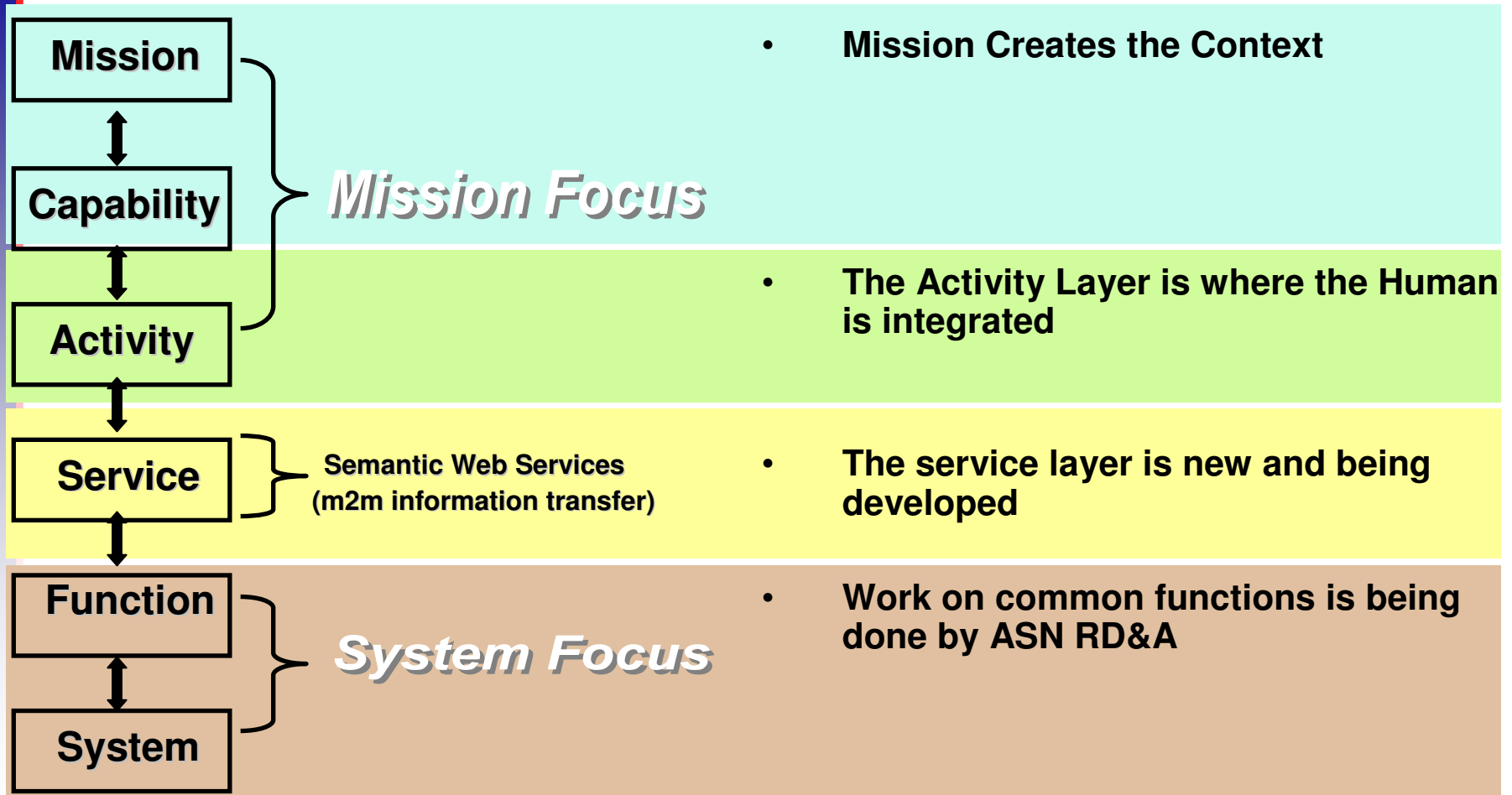
Ontology: An Enabling Technology

- **We will focus the aspects of Data Understandability and the development of shared meaning**

- **Ontology – An Enabling Technology**

  - **An ontology models the vocabulary and meaning of data domains**
  - **Objects in the domains and relationships among objects**
  - **Properties, function and processes involving those objects**
  - **Constraints and rules about the objects**
  - **Defines a Core Lexicon, Taxonomy, data dictionary, data schema**
  - **Ontologies permit fine, accurate, consistent, meaningful distinctions to be made between classes, instances, properties, attributes and relations in the data domain.**

Mission Context

- **Mission Context allows the user to use data to complete their mission**

- **Mission completion and the information for that completion is the central concept**

- **The MDA Data framework has to capture the data requirements, guidelines, and procedures for Mission Completion**

Ontologies will Implement our Context

Information Flow Stack

Mission

Capability

Activity

Mission Focus

Service

Semantic Web Services
(m2m information transfer)

Function

System

System Focus

- **Mission Creates the Context**

- **The Activity Layer is where the Human is integrated**

- **The service layer is new and being developed**

- **Work on common functions is being done by ASN RD&A**

Ontologies Development

Attributes

Who, How, What, Where, When, Why	**Mission**
" " " " " "	**Capability**
" " " " " "	**Activity**
" " " " " "	**Service**
" " " " " "	**Function**
" " " " " "	**System**

Mission, Capability, Activity → **Mission Ontology**

Service → **Semantic Web Services (m2m information transfer)**

Function, System → **Instance Ontologies**
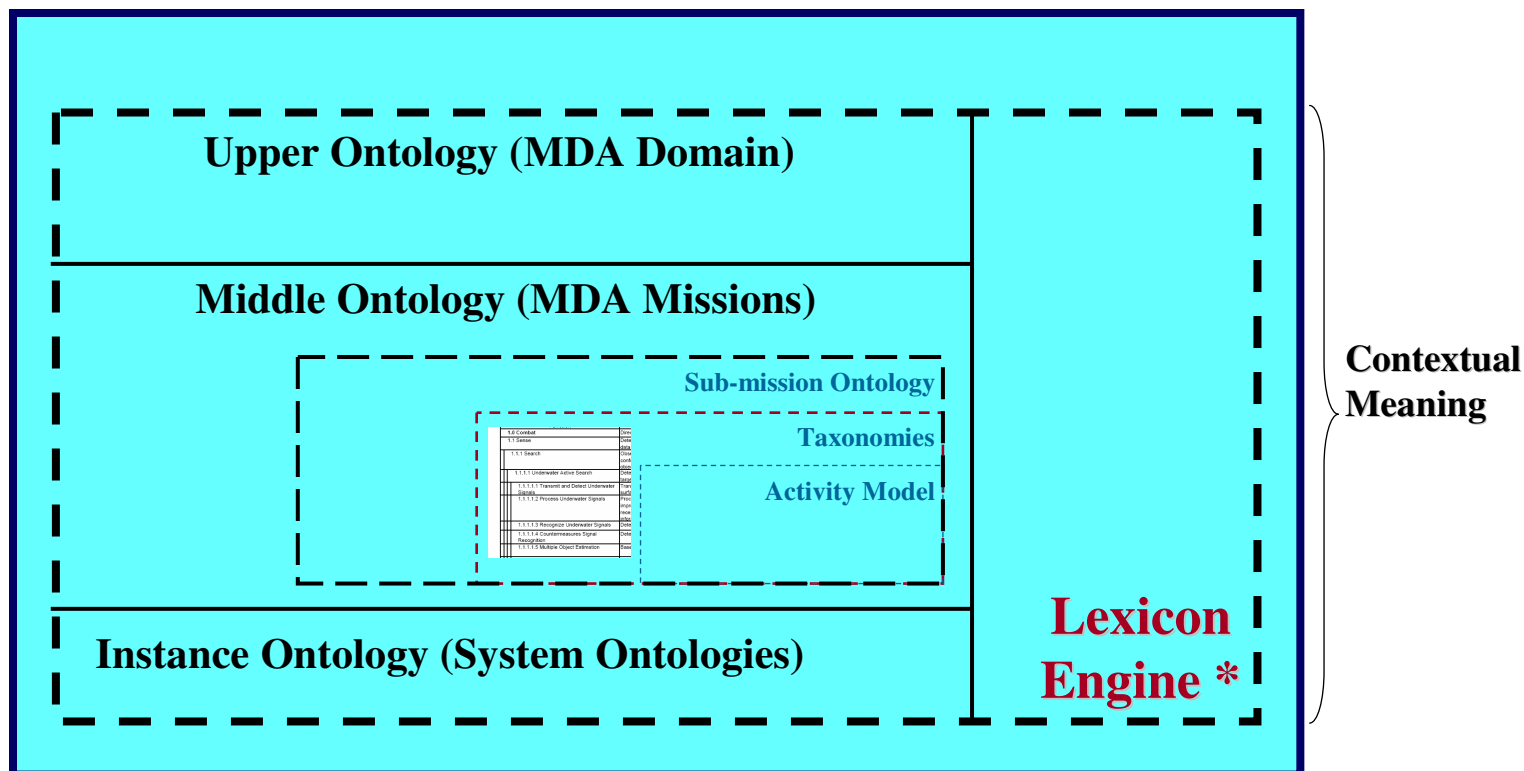
- Workload Element Library
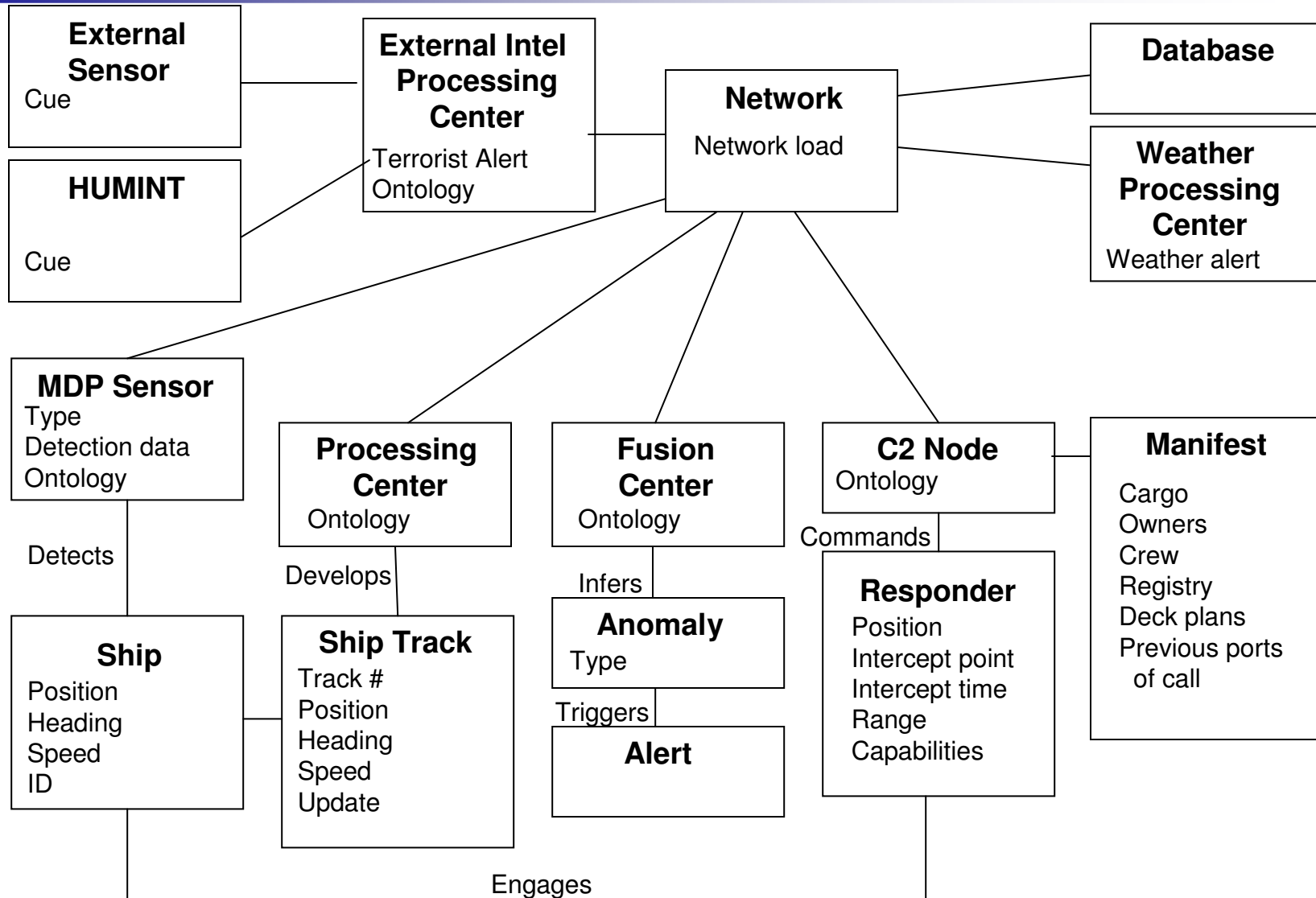- Skill Object
- System Design Task
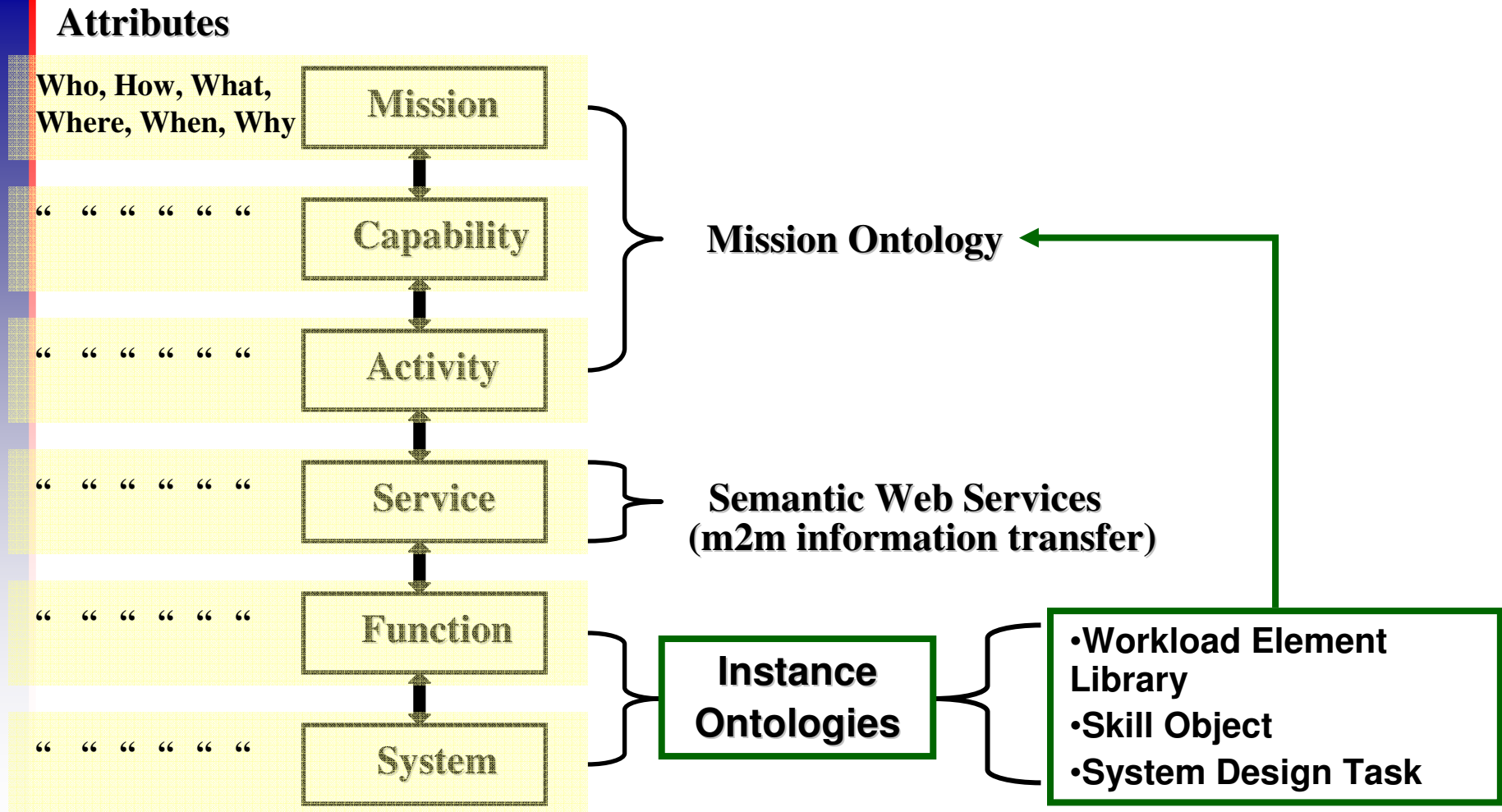
* Derived from the Navy Semantic Working Group proceedings, 27 July 2005, MITRE, San Diego, chaired by Brad Mercer and contributions by Paul Shaw
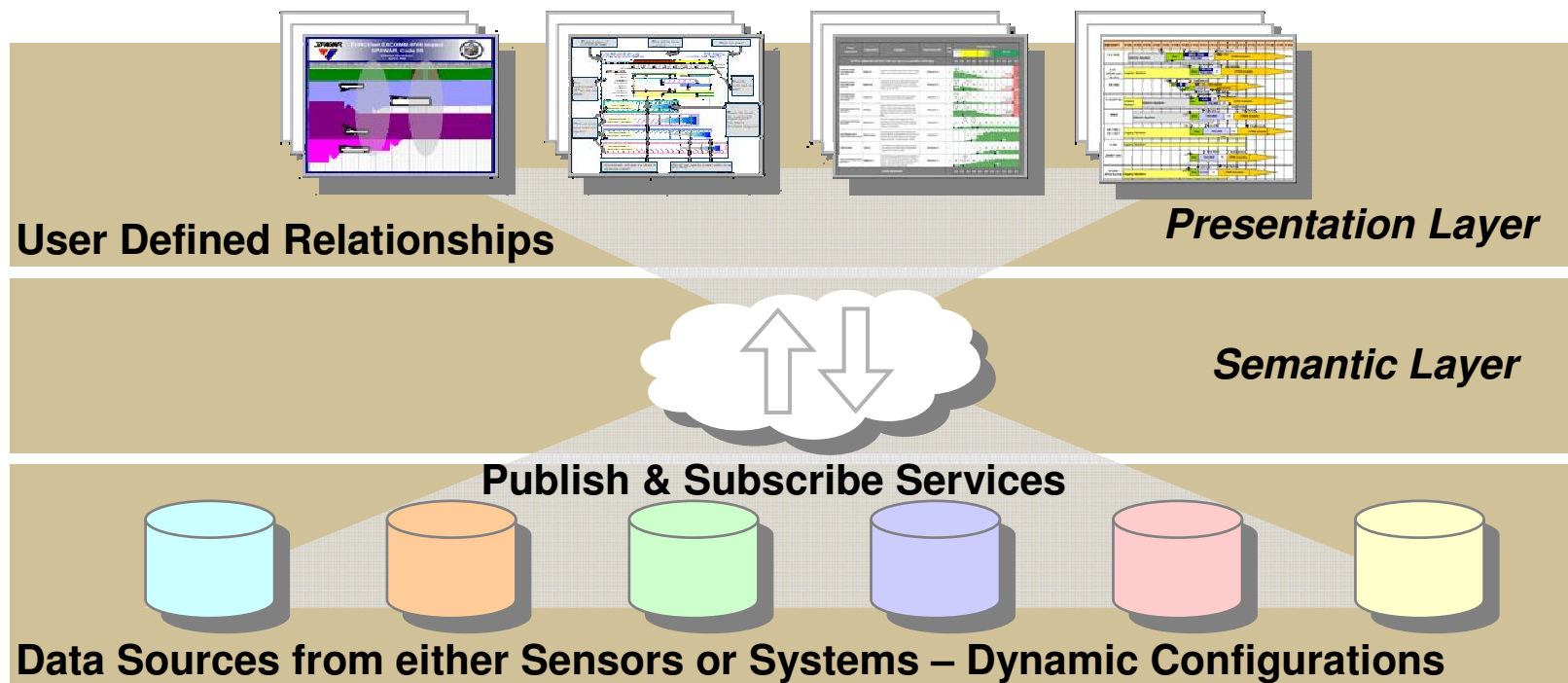
Ontology Framework

Note: Ontological Layers are frequently discussed by W3C. The DON CIO Technology eXchange Clearinghouse (a Navy Semantic Web Project) uses this layering and lexicon engine.

Sample Concept Diagram

External Sensor

Cue

HUMINT

Cue

External Intel Processing Center

Terrorist Alert
Ontology

Network

Network load

Database

Weather Processing Center

Weather alert

MDP Sensor
Type
Detection data
Ontology

Detects

Processing Center

Ontology

Develops

Fusion Center

Ontology

Infers

C2 Node
Ontology

Commands

Manifest

Cargo
Owners
Crew
Registry
Deck plans
Previous ports
  of call

Ship
Position
Heading
Speed
ID

Ship Track
Track #
Position
Heading
Speed
Update

Anomaly
Type

Triggers

Alert

Responder
Position
Intercept point
Intercept time
Range
Capabilities

Engages

MDA Data Fusion

- Reduced Need for Point to Point Interoperability
  - Publish and Subscribe Enabled for Use
    - Dynamic Communities of Interest

User Defined Relationships

Presentation Layer

Semantic Layer

Publish & Subscribe Services

Data Sources from either Sensors or Systems – Dynamic Configurations

Semantics of Security

- **The MDA Data in a Net Centric Environment Poses New, Exciting Challenges**

- **The MDA "Missions" Provides the Necessary Context for our Data**

- **Technologies like the Semantic Web with the use of Ontologies are Key enabler for the achievement of our MDA Objectives**